NATIONAL
PROTECTION
CENTER

August 10, 1998

MEMORANDUM

From:

NCIS

TO:

CIU Chief

SSA

Subj:

WRIGHT PATTERSON AIR FORCE BASE

VICTIM; CITA - COMPUTER INTRUSION

288-CI-NEW

1. As requested by I forwarded a request to the Fleet Intelligence Warfare Center (FIWC) to provide all information relating to the following Russian ISPs:

Cityline.ru

Microdin.ru

Sovam.com

Orc.ru

Demos.net

Demos.su

64C

Additionally, the following passwords and tools/usernames were researched:

Passwords:



Tools/usernames:



2. Attached are the results of a search of FIWC's database. The FIWC will report any additional information pertinent to this tasking as it becomes available.



10 August 1998

The following pages pertain to the Russian Internet addresses you provided. I have also included the incidents that we have seen from those sites.

We don't have any information in our database on the passwords "" and nor do we have any information on the usernames "" Additionally, we have no information regarding the files that were stolen from right-Patterson AFB. We don't monitor the IRC, so I can't answer the question regarding anyone bragging about this activity. Lastly, we don't have enough information to determine if this hacking style is similar to other hacks. There's nothing in our database to indicate any similarities.

Regarding the other known threats using x windows, the following is provided:

There are three major areas to look at when talking about security concerns with a X-Windows system. The first is access control. The "xhost" command denys remote connectios to an xserver. An improper configured x-server would allow an unauthorized user to watch key strokes, grab copies of window on the local system, or even export displays onto themisconfigured box. The second concern is connections to the the x-server. In order to connect to the server to tell it to export x displays, a user must log into it via a shell (flogin, rsh, telnet, or ssh). Most protocols don't use encryption and the login could be sniffed. This would allow a hacker to use a valid account and use an X system for their own purposes. The last concern is buffer overruns. A hacker would exploit a buffer overun by tasking the x-application with input it was not designed to handle. The user would then have shell access equivalent to the access the process was running at. If the program was setuid to run as root for everybody, then the hacker has root access! All three of the concerns can be address and handled. The access control problem is simple. A command of "xhost -" denies anyone access. Then access can be granted for those that absolutely need it. The unencrypted logging can be solved by using a securelogin method like secure shell. The buffer overruns are a bit harder to get a hold of. These type of exploits range from operation system to operating system. The system administrator of the network needs to know the different . operating systems and check the vendor pages for alerts and paths on a routine basis. These precautions keep the security risks associated with this service under control.

I hope this information is useful and what you need. Please let me know if there is anything else I can do.

cityline.ru

Name: nal.cityline.ru

Address:

inetnum:

netname: CITYLINERU

descr: Cityline offers dial-up and leased line access to Internet

descr: for Moscow and St.Peterburg regions.

country: RU

admin-c: AD705-RIPE tech-c: MB427-RIPE status: ASSIGNED PA

notify: Error! Bookmark not defined.

mnt-by: CITYLINERU-MNT

source: RIPE

routed

descr: Cityline offers dial-up and leased line access to Internet

descr: for Moscow and St.Peterburg regions.

origin: AS8498

notify: Error! Bookmark not defined.

mut-by: CITYLINERU-MNT

source: RIPE

person:

address: Cityline

address:

address:

phone:

fax-no: +7 095 245 8877

e-mail: Error! Bookmark not defined.

nic-hdl: AD705-RIPE

notify: Error! Bookmark not defined.

source: RIPE

person:

address:

address: address:

phone:

e-mail: Error! Bookmark not defined.

nic-hdl: MB427-RIPE

source: RIPE

67E

13C

(1)

microdin.ru (NAVCIRT Incident 98-5 of 6Jan98)

Name: microdin.ru

Address:

inemum:

netname: MICRONET descr: MicroNet Ltd.

descr: Requested network ip numbers will be used for connecting

descr: to MAcomnet.

country: RU

admin-c: SB1164-RIPE tech-c: DV86-RIPE status: ASSIGNED PA

notify: Error! Bookmark not defined.

source: RIPE

route:

descr: Micronet Ltd.

descr: 18 Novozavodskaya st descr: Moscow Russia 121309

origin: AS8470

notify: Error! Bookmark not defined. notify: Error! Bookmark not defined.

mnt-by: MACOMNET-MNT

source: RIPE

person:

address: MicroNet Ltd.

address: 18, Novozavodskayast address: 121309, Moscow, Russia

phone: +7 095 145-9520 phone: +7 095 145-9522 phone: +7 095 142-0618 fax-no: +7 095 924-0464

e-mail: Error! Bookmark not defined.

nic-hdl: SB1164-RIPE

source: RIPE

person:

address: address:

phone: e-mail: Error! Bookmark not defined.

nic-hdl: DV86-RIPE source: RIPE **L**

670



sovam.com

sovam.com preference = 200, mail exchanger = relay2.sovam.com

sovam.com preference = 100, mail exchanger = relay1.sovam.com

sovam.com nameserver = ns2.sovam.com

sovam.com nameserver = nic.near.net

sovam.com nameserver = pandora.sf.ca.us

sovam.com nameserver = ns.sovam.com

relay2.sovam.com internet address =

relay1.sovam.com internet address =

ns2.sovam.com internet address =

nic.near.net internet address = pandora.sf.ca.us internet address =

ns.sovam.com internet address =

[rs.internic.net]

Registrant

Sovam Teleport (SOV AM-DOM)

2A Nezhdanova st

Moscow, Russia 109003

RU

Domain Name: SOVAM.COM

Administrative Contact:

(KA41) Error! Bookmark not defined.

Technical Contact, Zone Contact:

Semenyuk, Igor (IS13) Error! Bookmark not defined.

Record last updated on 19-Mar-98.

Record created on 22-Jan-93.

Database last updated on 6-Aug-98 04:06:34 EDT.

Domain servers in listed order:

NS.SOVAM.COM

NIC.NEAR.NET

inetnum:

netname:

descr. Sovam Teleport

descr: Moscow, Russia

country: RU

admin-c: AK57-RIPE

tech-c: IS13

rev-srv: ns.sovam.com

rev-srv: ns2.sovam.com

rev-srv: nic.near.net

3

status: ASSIGNED PA

notify: Error! Bookmark not defined.

mnt-by: AS3216-MNT

source: RIPE

route:

376 descr: SOVAM DELEGATED BLOCK-I

origin: AS3216

advisory: AS690 1:3561 2:1128 notify: Error! Bookmark not defined.

mnt-by: AS3216-MNT

source: RIPE

person:

address: SOVAM TELEPORT Company Ltd.

address: address:

address:

phone:

fax-no: +/ 093 4384133

e-mail: Error! Bookmark not defined.

nic-hdl: AK57-RIPE

source: RIPE

67C

person: address: SOVAM TELEPORT Company Ltd.

address: address:

addressi phone:

phone:

fax-no: +7 095 2584133

e-mail: Error! Bookmark not defined.

nic-hdl: IS13 source: RIPE



orc.ru

orc.ru preference = 20, mail exchanger = mail2.ras.ru
orc.ru preference = 5, mail exchanger = mail.orc.ru
orc.ru preference = 10, mail exchanger = mail1.orc.ru
orc.ru preference = 15, mail exchanger = mail1.orc.ru
orc.ru nameserver = ns.orc.ru
orc.ru nameserver = nss.orc.ru
orc.ru nameserver = nss.orc.ru
orc.ru nameserver = nss.msu.ru
mail2.ras.ru internet address =
mail1.orc.ru internet address =
ns.orc.ru internet address =
nss.orc.ru internet address =

[n.internic.net] [No name] (NS31095-HST)

nss.msu.ru internet address =

67C

Hostnama: NS,ORC.RU

Address:

System: ? running ?

Coordinator:

CAH30) Error! Bookmark not defined.

Record last updated on 18-Sep-97.

Database last updated on 6-Aug-98 04:06:34 EDT.

demos.net (Navcirt 98-6211 of 3 Aug 98)
demos.net preference = 50, mail exchanger = relay1.demos.su
demos.net preference = 100, mail exchanger = relay2.demos.su
demos.net nameserver = ns.demos.su
demos.net nameserver = ns1.demos.net
relay1.demos.su internet address =
relay2.demos.su internet address =
ns.demos.su internet address =
ns.demos.su internet address =
ns.demos.su internet address =
ns.demos.net internet address =
s.demos.net internet address =
s.demo

17E

inetnum:

netname: DEMOS-CORP

descr: DEMOS Corporate Network

(5)

descr: Demos Plus Co. Ltd. descr: Moscow, Russia

country: RU admin-c: PA75 tech-c: ED12-RIPE tech-c: GB90-RIPE tech-c: GK41-RIPE mit-by: AS2578-MNT

source: RIPE

PE 67 8

route:

descr. DEMOS origin: AS2578

notify: Error! Bookmark not defined.

mnt-by: AS2578-MNT

source: RIPE

person:

address: Demos Plus Ltd.

address: Ovchinnikovskaya nab. 6/1

address: Moscow 113035

address: Russia

phone: +7 095 9566233 phone: +7 095 9566234 fax-no: +7 095 9565042

e-mail: Error! Bookmark not defined.

nic-hdl: PA75 source: RIPE

person:

address: Demos Company Ltd.
address: 6-1 Ovchinnikovskaya nab.

address: Moscow 113035

address: Russia

phone: +7 095 956 6233 phone: +7 095 956 6234 fax-no: +7 095 233 5016

e-mail: Error! Bookmark not defined.

nic-hdl: ED12-RIPE

notify: Error! Bookmark not defined.

source: RIPE

ملط

.

6

demos.su

demos.su preference = 100, mail exchanger = relay2.demos.su demos.su preference = 50, mail exchanger = relay1.demos.su

demos.su nameserver = ns.demos.su demos.su nameserver = nsl.demos.net

dismos.su nameserver = ns.ussr.eu.net

relay2.demos.su internet address =

relay I.demos.su internet address = na.demos.su internet address

ns.demos.su internet address =

ns i .demos.net internet address = ns.ussr.eu.net internet address =



% Rights restricted by copyright. See Error! Bookmark not defined.

inetnum:

netname: RU-DEMOS-970415

descr: PROVIDER

descr: Demos Company Ltd.

country: RU

admin-c: ED12-RIPE admin-c: AAP1-RIPE tech-c: SL6-RIPE tech-c: OB36-RIPE status: ALLOCATED PA

mnt-by: RIPE-NCC-HM-MNT

source: RIPE -

routes

descr. DEMOS origin: AS2578

notify: Error! Bookmark not defined.

mnt-by: AS2578-MNT

source: RIPE

person:

address: Demos Company Ltd. address: 6-1 Ovchinnikovskaya nab.

address: Moscow 113035

address: Russia

phone: +7 095 956 6233 phone: +7 095 956 6234 fax-no: +7 095 233 5016

e-mail: Error! Bookmark not defined.

nic-hdl: ED12-RIPE

notify: Error! Bookmark not defined.

source: RIPE



person:

address: Russian Institute for Public Networks

address: 1, Kurchatov sq address: Moscow address: Russis

phone: +7 095 1967278 fax-no: +7 095 1964984

e-mail: Error! Bookmark not defined.

nic-hdl: AAP1-RIPE

remarks: Admia contact for SU comain

ramarks: xSU/RU NIC contact

source: RIPE

person:

address: Russian Institute for Public Networks

address: 1 Kurchatov square address: 123182 Moscow

address: Russia

phone: +7 095 196 7363 fax-no: +7 095 196 4984

e-mail: Error! Bookmark not defined.

nic-hdl: SL6-RIPE source: RIPE

person:

address: Russian Institute for Public Networks

address: 1 Kurchatov square address: 123182 Moscow

address: Russia

phone: +7 095 192 7933 fax-no: +7 095 946 9841

e-mail: Error! Bookmark not defined.

nic-hdl: OB36-RIPE

notify: Error! Bookmark not defined.

source: RIPE

67C



IP Incident hits:

cityline.ru



microdin.ru



67E

sovam.com



orc.ru

no hits on old database (to mid Jul 1998)

demos.net



demos.su

no hits on old database (to mid Jul 1998)